UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,621	10/30/2003	Makoto Fujiwara	60188-694	5601

7590 07/30/2007

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/696,621	FUJIWARA ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see att*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's election of claims 1-8 in the reply filed on 5/4/2007 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement or indicated whether the election is with or without traverse, the election has been treated as an election without traverse (MPEP § 818.03(a)). Claims 1-8 are presented for examination.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 10/30/2003, 3/9/2004, and 5/2/2007 has been reviewed by the Examiner.

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686

F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4.1 Claims 1-8 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-17 of copending Application No. 10/624,481. Although the conflicting claims are not identical, they are not patentably distinct from each other because for instance the difference between claim 1 of the present application and claims 10 and 12 of the copending application is that the copending application is silent about receiving the common key-encrypted program from a server. However in claim 12 of the copending application there is suggestion that the encrypted program is supplied from an external memory. Therefore, it would have been obvious to one of ordinary skill in the art to supply the encrypted program from a server because since the program is program distribution is common practice in the art and it would have required only routine skill in the art to modify the copending application using a server as external memory to have the program supplied from another computer such as a server.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

4.2 Claims 1-8 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-20 of copending Application No. 10/654,084. Although the conflicting claims are not identical, they are not patentably distinct from each other because the difference between claim 1 of the present application and claims 19-20 of the copending application is that the copending application is silent about receiving the common key-encrypted program from a server. However in claim 19 of the copending application there is suggestion that the encrypted program is stored in an external memory. Therefore, it would have been obvious to one of ordinary skill in the art to supply the encrypted program from a server because since the program is program distribution is common practice in the art and it would have required only routine skill in the art to modify the copending application using a server as external memory to have the program supplied from another computer such as a server.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the

international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,970,565 to **Rindsberg**.

As per claim 1, **Rindsberg** discloses a method for updating an inherent key-encrypted program in a system including an LSI device and an external memory, the inherent key-encrypted program being generated by encryption with an inherent key unique to the LSI device and being stored in the external memory, the method comprising:
downloading and installing an encrypted patch program encrypted by a shared key transmitted by satellite (see column 7, lines 23-32) that meets the recitation of a first step of receiving by the system a common key-encrypted program (encrypted patch) generated by encryption with a common key (shared key) and transmitted from a server (see column 8, lines 4-10); it is implicit or inherent that a server transmits/broadcasts the program by satellite. **Rindsberg** discloses a second step of decrypting by the system the received common key- encrypted program to generate a raw program (see column 8, lines 12-16); and a third step of re-encrypting by the system the raw program with the inherent key (unique key) and storing the re-encrypted program in the external memory as a new inherent key-encrypted program (see column 8, lines 23-34).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 4, 6, and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,970,565 to **Rindsberg** in view of US Patent 6,577,734 to **Etzel et al**.

As per claim 2, **Rindsberg** substantially teaches the claimed method of claim 1. **Rindsberg** does not explicitly disclose receiving by the system common key information transmitted from the server and generating by the system a raw common key using the received common key information. **Etzel et al** in an analogous art discloses receiving by a device shared key information transmitted from system 100 and generating a shared key using the shared key information (see column 6, lines 6-20) that meets the recitation of receiving by the system common key information transmitted from the server and generating by the system a raw common key using the received common key information and further discloses wherein at the second step, the raw common key is used to decrypt the common key-encrypted program (see column 7, lines 39-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rindsberg** to allow each device to generate own shared key from common key information as taught by **Etzel et al** because it would avoid transmission of the key and thereby preventing the key to be obtained by unauthorized party as suggested by **Rindsberg** (see **Rindsberg**, column 7, lines 44-50).

As per claim 4, **Rindsberg** substantially teaches the claimed method of claim 1. **Rindsberg** discloses that each unique key (inherent key) corresponds to a unique ID and extracted upon reset (bootup) (see column 7, lines 33-41) and further discloses the raw inherent key is used for re-encrypting the raw program (see column 7, lines 36-38). **Rindsberg** does not explicitly disclose that the unique key is generated upon reset. **Etzel et al** in an analogous art discloses during booting generating a unique device key using device key information and stored in its secure memory to prevent tampering (see column 3, lines 12-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rindsberg** to allow each device to generate unique device key upon startup using inherent key information as taught by **Etzel et al** so as to securely manage the keys and prevent them from being misappropriated for fraudulent purposes (see **Etzel et al,** column 1, lines 47-50).

As per claim 6, the combination of **Rindsberg** and **Etzel et al** discloses wherein the generated raw inherent key is stored in a register of the LSI device and is used for decrypting the inherent key-encrypted program to a raw program for execution of the inherent key-encrypted program (see **Rindsberg**, column 8, lines 52-54).

As per claim 7, the combination of **Rindsberg** and **Etzel et al** discloses the LSI device includes a boot ROM in which a boot program is stored (see **Rindsberg**, column 7, lines 7-21) and (see **Etzel et al**, column 9, lines 20-34); **Rindsberg** discloses external memory interface 71 and additional interfaces or communication link and receiver for establishing data transmission

with the server (see figures 2 and 5 and column 7, lines 44-50 and column 9, lines 23-38) that meets the recitation of external memory includes an acquisition program for establishing data transmission between the LSI device and a server **Rindsberg** also discloses controlling update processing performed after the reception of the common key-encrypted program based on the boot program stored in the boot ROM (see column 6, line 54 through column 7, line 12) (see also **Etzel et al**, column 9, lines 20-30 and lines 50-63).

7. **Claims 3** and **5** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,970,565 to **Rindsberg** in view of US Patent 6,577,734 to **Etzel et al** as applied to claims 1-2 and further in view of US Patent Publication US 2002/0116632 to **Itoh et al** *(Applicant's IDS).*

As per claim 3, the combination of **Rindsberg** and **Etzel et al** discloses the claimed method of claim 2. Neither of the references explicitly discloses double encryption. **Itoh et al** in an analogous art discloses an encrypted common key generated by encrypting software key Ksoft with Ks2 and Ks2 generated by encrypting Ks2 with Ks1 (see page 6, paragraphs 93-95) that meets the recitation of wherein the common key information includes an encrypted common key generated by encrypting the raw common key with a raw first intermediate key, and an encrypted first intermediate key generated by encrypting the raw first intermediate key with a raw second intermediate key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a double encrypted key as taught by allow each device to generate own shared key from common

key information as taught by **Itoh et al** because having the software key dependent on two keys in a double encryption method would make the key less vulnerable against tampering.

As per claim 5, the combination of **Rindsberg** and **Etzel et al** discloses the claimed method of claim 4. Claim 5 is similar to claim 3 except for double encrypting the raw inherent key whereas claim 3 double encrypts the raw common key. **Itoh et al** discloses double encryption as shown in claim 3 above. Therefore, claim 5 is rejected on the same rationale as the rejection of claim 3 above.

8. **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,970,565 to **Rindsberg.**

As per claim 8, **Rindsberg** substantially teaches performing an integrity check on the decrypted patch program (see column 8, lines 12-18) that meets the recitation of wherein at the second step, the received HASH value is used to perform a HASH verification on the decrypted raw program. **Rindsberg** is silent about the hash value is received. It is apparent to one of ordinary skill in the art that an integrity check in cryptography is performed using hashing algorithms and to verify that the present state of data has not been tampered or modified and that it was received correctly without error as suggested by **Rindsberg,** it must be compared with either a value received or stored. Therefore, based on common knowledge in the art of cryptography this modification would have been obvious to one of ordinary skill in the art and would not be patentably distinct from the invention disclosed by **Rindsberg**.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses different cryptographic algorithms such as re-encryption and double encryption methods. (See PTO-form 892).

9.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Patent Examiner, A.U. 2136
July 22, 2007